FortiAnalyzer Upgrade Guide

VERSION 5.0.10

FORTINET

1

How to Upgrade

STEP 1: Backup Your Device.
Backup your device and its configuration.

STEP 2: Download.
Upgrade images are available from the Customer Support website.

STEP 3: Upgrade and Monitor.
Install the new firmware.

STEP 4: Verify and Validate.
Use the GUI to verify that the upgrade succeeded, and run the dataset validation tool to verify your datasets.

STEP 5: Convert Log Array to HA Clusters.
If Log Arrays are used to manage HA clusters in previous versions, you will need to convert them to HA clusters.

To upgrade from v5.0.6 to v5.0.10:
Watch the following video
http://forti.net/faz_upgrade

2

Upgrade Paths

IMPORTANT: FortiAnalyzer must be running v5.0.6 or later before upgrading to FortiAnalyzer v5.0.10.

Initial Version	Upgrade To	Log Database Rebuild Required?
≤ 5.0.5	5.0.6	Yes
5.0.6	5.0.10	Yes
5.0.7	5.0.10	No
5.0.8	5.0.10	No
5.0.9	5.0.10	No

3

Detailed Upgrade Instructions

Step 1. Back Up Your Device.

Backup your device configuration from the Systems Settings tab.

Step 2. Download.

Download your firmware image.

1. Use the CLI command to check for current reports. Allow them to complete prior to upgrading.

```
FAZ1000D # dia report status running
FAZ1000D # dia report status pending
```

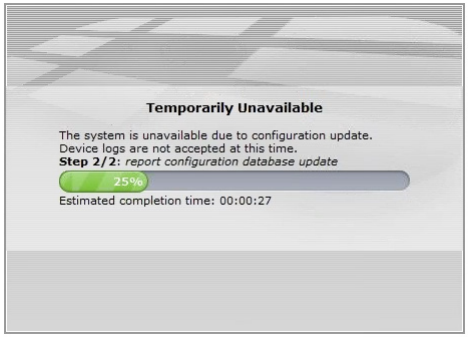
2. If you are upgrading a FortiAnalyzer VM, make sure your VM partition has more than 512MB*, and your VM server is up to date.

It is recommended to allocate 1024MB for the FortiAnalyzer VM partition.

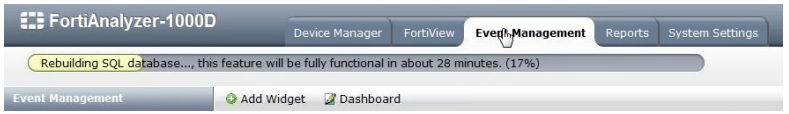
Step 3. Upgrade and Monitor

Install the downloaded firmware image.

During a firmware upgrade, you will temporarily disconnect to your FortiAnalyzer. When the firmware has been installed, you can reconnect to your device.

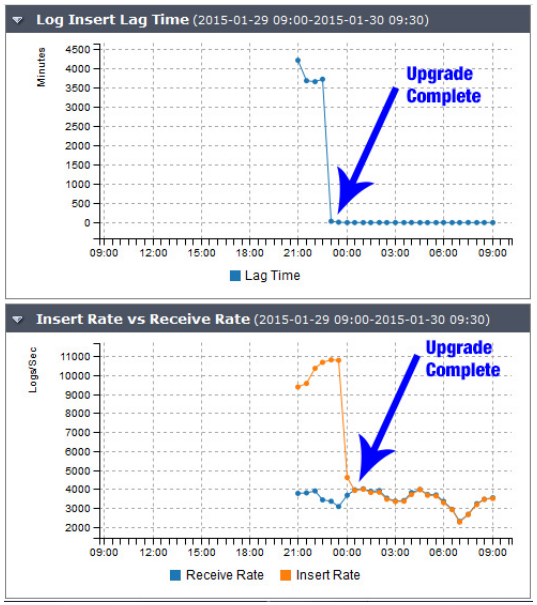


When complete, you will be able to log in and access your FortiAnalyzer. Not all features will be available immediately while the SQL database is rebuilt. A status bar will keep you up to date on the rebuild status.



Step 3. Upgrade and Monitor

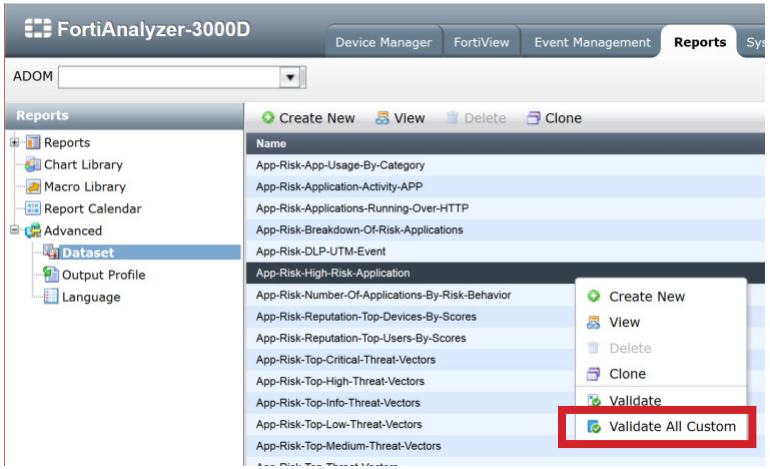
Monitor the rebuild progress with the *Log Insert Lag Time* and *Insert Rate vs Receive Rate* widgets. These widgets will show you the gap between logs being received and logs being inserted after the upgrade. You can customize this widget to show data every 60 to 240 seconds. As shown below, you will notice an initial delay in logs being inserted, but that will resolve itself as time passes. You can add these widgets in the same way you add other widgets in the Dashboard.

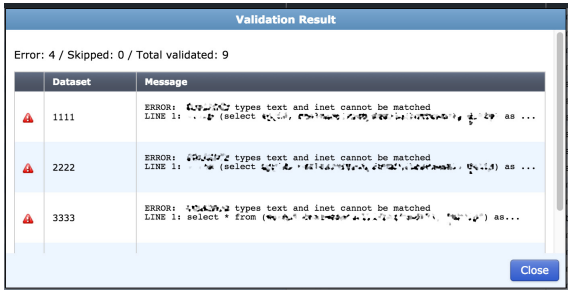


Step 4. Verify and Validate

After using GUI to verify that the upgrade succeeded, run dataset validation tool to verify your datasets.

1. Select the *Reports* tab.
2. Select *Advanced* in the left pane.
3. Select *Dataset*.
4. Right-click any report and select *Validate All Custom*.



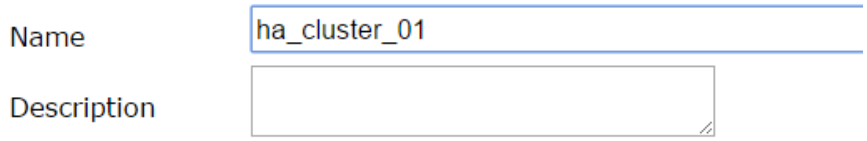


Step 5. HA Cluster for Log Conversion

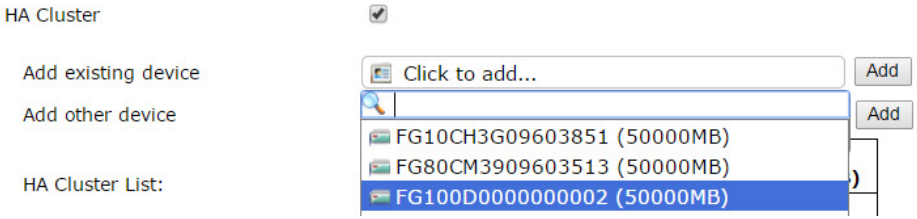
If you have been using log array to manage your HA device disk quota, migrate from log array to HA cluster for easier management.

Follow the steps below to migrate from log array to HA cluster.

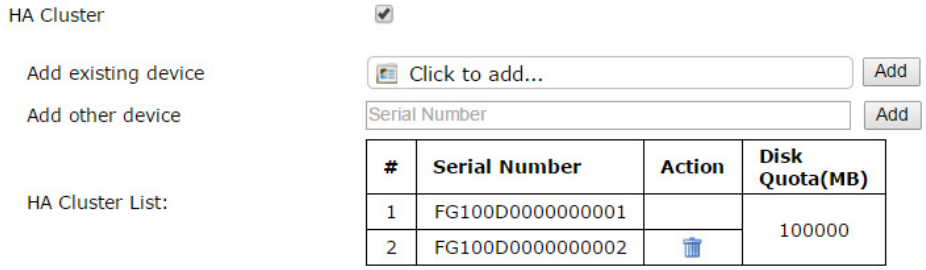
1. In the Device & Groups tab, create a new entry for the HA device by right-clicking on one of the member devices.
2. Select *Edit* and name the entry as `ha_cluster_01`.



3. Check the HA Cluster option box. In the *Add Other Device* field, select other member devices from the drop down menu. Click Add.



4. Once added, the HA Cluster List will show all member devices with the disk quota assigned to the cluster instead of each individual device. You can change the disk quota based on your requirements.



5. Select *OK* and observe the HA cluster is now added. The cluster can be identified by the HA cluster icon.

Do not delete the other device yet. You will lose all your data.

CLI Commands

In order to complete the HA cluster, the logs of all the member devices need to be moved to the HA cluster.

1. Run `diagnose log device` to show `ha_cluster_01`.

2. Run `#execute log device logstore list` to list the member devices.

```
FAZ1000C # diagnose log device
Device Name       Device ID
HA_Cluster_01     FGHA001206932942_CID
          |- HA cluster member: FG100D0000000001
          |- HA cluster member: FG100D0000000002
```

```
FAZ1000C # execute log device logstore list
Device ID                      log files
=======================================================
(1) FG100D0000000001    N/A        N/A    zombie
(2) FGHA001206932942_CID           0MB          0MB
(3) FG100D0000000002    N/A        N/A    zombie
```

3. `#execute log device logstore move`†‡ `<source> <destination>`

```
FAZ1000C # execute log device logstore move
FG100D0000000001 FGHA001206932942_CID
```

Example: Source: FG100Dxxx1 (individual devices)
Destination: FGHA001xxxx_CID (HA cluster)

†You may need extra temporary free disk space equivalent to the log size to be able to move them.
‡The time to complete the log move and database rebuild is determined by the log size.

This command is necessary for each individual device being added to the HA cluster.

After all the member device logs have been moved into the HA cluster. You can delete the individual devices from the GUI under the Device & Group tab.

4. Run `#execute log device logstore clear All` to clean up all log files and archives.

```
FAZ1000C # execute log device logstore clear All
This will clean up all zombie devices logs and
archive files.
Do you want to continue? (y/n)y
```

5. Run `#execute sql-local rebuild-db` to complete the log migration into the HA cluster.

```
FAZ1000C # execute sql-local rebuild-db
Rebuild the whole SQL database has been requested.
This operation will remove the SQL database and
rebuild from log data.
This operation will reboot the device.
Do you want to continue? (y/n)y
```

6. You can now delete the log array from the GUI. Go Fortiview > Log View > Tools > Manage Log Arrays> select *Delete*.

Supported Models

The following models support upgrading to FortiAnalyzer v5.0.10:

FAZ-100C
FAZ-200D
FAZ-300D
FAZ-400B
FAZ-400C
FAZ-1000B
FAZ-1000C
FAZ-1000D
FAZ-2000A
FAZ-2000B
FAZ-3000D
FAZ-3000E
FAZ-3500E
FAZ-4000A
FAZ-4000B

FAZ-VM32
FAZ-VM64
FAZ-VM64-AWS
FAZ-VM64-HV
FAZ-VM64-KVM
FAZ-VM64-XEN

FORTINET